

DOCKET NUMBER: YO999-002

1 **CLAIMS**

2 What is claimed is:

3 1. A method for achieving client to server end to end
4 security guarantees, the method comprising:

5 employing a proxy between the client and the
6 server to provide connection links between the client
7 and the server;

8 embedding a secure coprocessor for use as an agent
9 of the client and/or the server;

10 the coprocessor acting as a converter between at
11 least one protocol the client supports and at least one
12 other protocol supported by the server; and

13 employing respective security protocols of said at
14 least one protocol and said at least one other
15 ~~protocol.~~

16 2. A method as recited ^a in claim 1, wherein the
17 coprocessor is located at the site of the proxy.

18 3. A method as recited in claim 1, further comprising
19 the step of the coprocessor ^a guaranteeing that an
20 application embedded in the coprocessor performs to a
21 degree of security proscribed by the client and/or
22 server.

DOCKET NUMBER: YO999-002

1 4. A method as recited in claim 1, further comprising
2 the coprocessor assuring that the proxy can not tamper
3 with the functioning of the agent.

4 5. A method as recited in claim 1, wherein the client
5 is a pervasive computing device.

6 6. A method as recited in claim 1, further comprising
7 the step of adapting content supplied by the client to
8 fit constraints of the server and/or the connection
9 links.

10 7. A method for providing secure communications on a
11 network, the method comprising;

12 securely embedding an agent at a proxy in the
13 network, and

14 splicing a plurality of secure communication
15 protocols of different protocol suites into the agent.

16 8. A method as recited in claim 7, wherein the step of
17 splicing includes splicing a security protocol of the
18 Wireless Applications Protocol suite (WAP) to that of
19 the Internet protocol (IP) suite.

20 9. A method as recited in claim 8, wherein the
21 Wireless Applications Protocol suite is used by a
22 pervasive computing device.

DOCKET NUMBER: YO999-002

1 10. A method as recited in claim 7, further comprising
2 the agent performing at least one content adaptation
3 function.

4 11. A method as recited in claim 10, wherein the step
5 of performing includes maintaining communication
6 privacy.

7 12. A method as recited in claim 7, further comprising
8 maintaining a state of a splicing process resulting
9 from the step of splicing.

10 13. A method as recited in claim 12, wherein the step
11 of maintaining includes employing a storage device
12 external to the proxy, and using cryptographic means to
13 encrypt the state.

14 14. A method for providing network security to a
15 network employing a proxy, the method comprising:

16 embedding a trusted application in a secure
17 coprocessor located at the site of a proxy; and

18 delegating to a networking infrastructure a task
19 of enforcing a trust model.

20 15. A method as recited in claim 14, further
21 comprising guaranteeing that the application is trusted

DOCKET NUMBER: YO999-002

1 to enforce the trust model between at least one server
2 and a plurality of clients.

3 16. A method as recited in claim 14, further
4 comprising assuring the tamper resistance of the
5 application.

6 17. A method for secure communication between a client
7 and a server employing an untrusted proxy; the method
8 comprising:

9 embedding a coprocessor at the proxy;

10 the proxy receiving a specific communication
11 request from a client;

12 the proxy forming an n-tuple for the specific
13 communication;

14 the proxy forwarding the n-tuple to the
15 coprocessor;

16 the coprocessor generating a response, including a
17 directive, to the n-tuple;

18 the coprocessor sending the response to the proxy;
19 and

20 the proxy implementing the directive.

DOCKET NUMBER: YO999-002

1 18. A method of claim 17, wherein the coprocessor is a
2 secure coprocessor.

3 19. A method of claim 17, wherein the step of
4 receiving includes:

5 awaiting a connection request from a client;

6 creating an entry in a storage module for the
7 client;

8 determining a sender of each received packet; and

9 retrieving a stored entry.

10 20. A method of claim 19, wherein the n-tuple includes
11 a sender id, an entry from a storage module and the
12 received packet.

13 21. A method of claim 17, wherein the client and the
14 server can be either a sender or a receiver, and the
15 step of generating includes employing a first protocol
16 from the sender to the proxy and a second protocol from
17 the proxy to the receiver and translating between the
18 said first and second protocols.

19 22. A method of claim 21, wherein the translating
20 includes decrypting the received packet as specified by
21 the security parameters negotiated as per the first
22 protocol and encrypting the decrypted packet as

DOCKET NUMBER: YO999-002

1 specified by the security parameters of the second
2 protocol.

3 23. A method of claim 21, wherein the translating
4 includes modifying the received packet to meet
5 constraints of the receiver and wherein the directive
6 includes forwarding to the receiver the packet
7 resulting from the step of modifying.

8 24. A method as recited in claim 23, further
9 comprising aggregating a plurality of packets into a
10 group of packets and performing content adaptation on
11 the group of packets.

12 25. A method of claim 17, wherein the communication
13 between the client and the proxy employ protocols
14 specified by the Wireless Application Protocol suite
15 [WAP].

16 26. A system to control security of a proxy
17 interconnecting a client to a server, the system
18 comprising:

19 a secure coprocessor used as an agent of the
20 client and/or the server; and

21 an application embedded in the coprocessor which
22 acts as a converter between at least one protocol the
23 client supports and at least other protocol supported
24 by the server, wherein the secure coprocessor employs

DOCKET NUMBER: YO999-002.

1 ~~respective security protocols of said at least one~~
2 ~~protocol and said at least one other protocol.~~

3 27. A system as recited in claim 26, wherein the
4 coprocessor is located at the site of the proxy.

5 28. A system as recited in claim 26, wherein the
6 coprocessor performs functions to guarantee that an
7 application embedded in the coprocessor performs to a
8 degree of security proscribed by the client and/or
9 server.

10 29. A system as recited in claim 26, wherein the
11 coprocessor functions to assure that the proxy can not
12 tamper with the functioning of the agent.

13 30. A system as recited in claim 26, wherein the
14 application embedded in the coprocessor adapts content
15 supplied by the server to fit constraints of the client
16 and the connection links.

17 31. A system as recited in claim 26, wherein the
18 application embedded in the coprocessor adapts content
19 supplied by the client to fit constraints of the server
20 and the connection links.

21 ~~32.~~ A system for providing network security to a
22 network employing a proxy, the system comprising:

DOCKET NUMBER: YO999-002

1 a secure coprocessor located at the site of a
2 proxy; and

3 a trusted application embedded in the coprocessor
4 wherein the coprocessor delegates the task of enforcing
5 an arbitrary trust model to the application.

6 33. A system as recited in claim 32, wherein the
7 coprocessor functions to guarantee that the application
8 is trusted to enforce the trust model between at least
9 one server and a plurality of clients.

10 34. A system as recited in claim 33, where the
11 coprocessor functions to assure the tamper resistance
12 of the application.

13 35. An article of manufacture comprising a computer
14 usable medium having computer readable program code
15 means embodied therein for achieving client to server
16 end to end security guarantees, the computer readable
17 program code means in said article of manufacture
18 comprising computer readable program code means for
19 causing a computer to effect:

20 employing a proxy between the client and the
21 server to provide connection links between the client
22 and the server;

23 embedding a secure coprocessor for use as an agent
24 of the client and/or the server;

4 employing respective security protocols of said at
5 least one protocol and said at least one other
6 protocol.

37. An article of manufacture as recited in claim 35,
the computer readable program code means in said
article of manufacture further comprising computer
readable program code means for causing a computer to
effect the coprocessor assuring that the proxy can not
tamper with the functioning of the agent.

~~Sub~~ 19
~~24~~ 20

DOCKET NUMBER: YO999-002

1 server to fit constraints of the client and/or the
2 connection links.

3 39. An article of manufacture as recited in claim 35,
4 the computer readable program code means in said
5 article of manufacture further comprising computer
6 readable program code means for causing a computer to
7 effect the step of adapting content supplied by the
8 client to fit constraints of the server and the
9 connection links.

10 40. A computer program product comprising a computer
11 usable medium having computer readable program code
12 means embodied therein for providing secure
13 communication on a network, the computer readable
14 program code means in said computer program product
15 comprising computer readable program code means for
16 causing a computer to effect:

17 securely embedding an agent at a proxy in the
18 network, and

19 splicing a plurality of secure communication
20 protocols of different protocol suites into the agent.

21 41. A computer program product as recited in claim 40,
22 wherein the step of splicing includes splicing a
23 security protocol of a Wireless Applications Protocol
24 suite (WAP) to that of the Internet protocol (IP)
25 suite.

DOCKET NUMBER: YO999-002

Sub 25
1 42. A computer program product as recited in claim 40,
2 wherein the splicing includes maintaining end to end
3 security guarantees without a modification at the
4 server.

5 43. A computer program product as recited in claim 40,
6 the computer readable program code means in said
7 computer program product further comprising computer
8 readable program code means for causing a computer to
9 effect the step of the agent performing at least one
10 content adaptation function.

11 44. A computer program product as recited in claim 40,
12 the computer readable program code means in said
13 computer program product further comprising computer
14 readable program code means for causing a computer to
15 effect the step of maintaining a state of a splicing
16 process resulting from the step of splicing.

17 45. A computer program product as recited in claim 44,
18 wherein the step of maintaining includes employing a
19 storage device external to the proxy, and using
20 cryptographic means to encrypt the state.

21 46. A computer program product comprising a computer
22 usable medium having computer readable program code
23 means embodied therein for providing network security
24 to a network employing a proxy, the computer readable
25 program code means in said computer program product

DOCKET NUMBER: YO999-002

1 comprising computer readable program code means for
2 causing a computer to effect the steps of:

3 embedding a trusted application in a secure
4 coprocessor located at the site of a proxy; and

5 delegating to a networking infrastructure a task
6 of enforcing a trust model.

7 47. A computer program product as recited in claim 46,
8 the computer readable program code means in said
9 computer program product further comprising computer
10 readable program code means for causing a computer to
11 effect the step of guaranteeing that the application is
12 trusted to enforce the trust model between at least one
13 server and a plurality of clients.

14 48. A computer program product as recited in claim 46,
15 the computer readable program code means in said
16 computer program product further comprising computer
17 readable program code means for causing a computer to
18 effect the step of assuring the tamper resistance of
19 the application.

20 ~~49.~~ A program storage device readable by machine,
21 tangibly embodying a program of instructions executable
22 by the machine to perform method steps for secure
23 communication between a client and a server employing
24 an untrusted proxy, said method steps comprising:

DOCKET NUMBER: YO999-002

1 embedding a coprocessor at the proxy;

2 the proxy receiving a specific communication
3 request from a client;

4 the proxy forming an n-tuple for the specific
5 communication;

6 the proxy forwarding the n-tuple to the
7 coprocessor;

8 the coprocessor generating a response, including a
9 directive, to the n-tuple; and

10 the coprocessor sending the response to the proxy;
11 and the proxy implementing the directive.

12 50. A program storage device readable by machine as
13 recited in claim 49, wherein the coprocessor is a
14 secure coprocessor.

15 51. A program storage device readable by machine as
16 recited in claim 49, wherein the step of receiving
17 includes:

18 awaiting a connection request from a first client;

19 creating an entry in a storage module for the
20 client;

DOCKET NUMBER: YO999-002

1 determining a sender of each received packet; and
2 retrieving a stored entry.

3 52. A program storage device readable by machine as
4 recited in claim 49, wherein the n-tuple includes a
5 sender id, an entry from a storage module and the
6 received packet.

7 53. A program storage device readable by machine as
8 recited in claim 49, wherein the client and the server
9 can be either a sender or a receiver, and the step of
10 generating includes employing a first protocol from the
11 sender to the proxy and a second protocol from the
12 proxy to the receiver and translating between the first
13 and second protocols.

14 54. A program storage device readable by machine as
15 recited in claim 49, wherein the translating includes
16 decrypting the received packet as specified by the
17 security parameters negotiated as per the first
18 protocol and encrypting the decrypted packet as
19 specified by the security parameters of the second
20 protocol.

21 55. A program storage device readable by machine as
22 recited in claim 53, wherein the translating includes
23 modifying the received packet to meet constraints of
24 the receiver and wherein the directive includes

20